IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/757,058
Filing Date ..... Jan. 8, 2001
Inventorship .....Brezak et al.
Applicant ..... Microsoft Corporation
Group Art Unit 2134
Examiner .....Tran, Ellen C.
Confirmation No. 6566
Attorney's Docket No. MS1-679US
Title: Credential Managment

To: Honorable Commissioner for Patents
Alexandria, VA 22313-1450

From: Emmanuel A. Rivera (Tel. 509-324-9256; Fax 509-323-8979)
Customer No. 22801

RESPONSE TO OCTOBER 19, 2005 NON-FINAL OFFICE ACTION

Sir:

In response to the office action (the Action) of **October 19, 2005**, the response is provided as follows:

Amendments to the specification begin on page 2 of this paper.

The listing of the claims begins on page 4 of this paper.

Remarks/Arguments begin on page 14 of this paper.

Amendments to the Specification

Please replace the paragraph at page 2, beginning at line 2 with the following:

A "credential" is a generic term for data used to verify the identity of an entity. An entity may be a server, a client, a service, etc. Typically, it is a user. Common forms of credentials include username/password model, X.509 Certificates, and bio-metric identification. There are two general types of credentials: Domain credentials and generic credentials.

Please replace the paragraphs at page 9, beginning at line 9 with the following:

A credential management module 152 is one such security process in the TCB 150. As its name implies, it manages the credentials of the computer 130. More specifically, it manages the credentials of each user of the computer 130.

Although not illustrated in Fig. 1, credential management module 152 may be composed multiple submodules. Some of these may be application-programming interfaces (APIs) that the applications may call to access credentials. More details about such APIs are provided in the "Exemplary Implementation employing APIs" section below. One or more other submodules may control the actual access of a user's credentials (including reads and writes) and control the encryption and decryption of credential databases, such as databases 154a-c. Herein, this submodule may be called the "credential management submodule."

Please replace the paragraph at page 9, beginning at line 22 with the following:

Fig. 1 illustrates multiple encrypted credential databases 154a-c with a graphical representation of a "user" associated with each database. This indicates that each database is associated with a particular user. The credentials for each user is collected and stored together within a database structure (e.g., databases 154a-c) associated with a specific user. That database is encrypted.

Please replace the paragraph at page 11, beginning at line 1 with the following:

Marshaling

Marshaling is the mechanism by which a description of a non-password credential can be passed to the TCB using an interface designed to support only password credentials. See the marshaling APIs, described in the "Exemplary Implementation employing APIs " section below, for details of an implementation that performs marshaling.